

Servium

an  advania company



KEEPING YOUR MICROSOFT 365 SECURE

The 7 protections that make
or break your cyber defences






While Microsoft 365 comes with some great cybersecurity tools, it can leave blind spots that go overlooked.

Naturally, Microsoft is continuously improving its security capabilities, but as a non-specialist cybersecurity vendor, notable gaps remain. Microsoft 365's protections depend on subscription levels, potentially compromising cybersecurity if subscriptions change for other reasons.

As a result, it's well worth reinforcing Microsoft's native protections with an additional layer of security that works alongside them - and that's exactly what Barracuda does. This guide covers 7 crucial protections you need to keep bad actors from compromising your Microsoft 365 defences, how well Microsoft's built-in measures deliver, and how Barracuda can help bolster your defences and keep your business and users secure.



...it's well worth reinforcing Microsoft's native protections with an additional layer of security.



The 7 protections that make or break your cyber defences

Your security, summarised

The table below provides a brief summary of which of the seven protections are offered by different Microsoft 365 licence tiers, helping you quickly identify where any gaps in your current defences may exist.

Feature	Microsoft 365 Licence						Notes
	Business Basic	Business Standard	Business Premium	E1	E3	E5	
Impersonation Protection Identifies senders that are impersonating legitimate users to protect against phishing and social engineering.	✗	✗	Disabled by default	✗	✗	Disabled by default	Included in MS Defender for Office 365 Plans 1 & 2
Microsoft 365 Data Backup Keeps your data secure and accessible to recover from attacks and other disruptions, even if Microsoft's production servers experience an outage.	✗	✗	✗	✗	✗	✗	High miss rate on threats - can be tuned to catch more, but results in many false positives
Zero-Day Attachment Sandboxing Opens attachments in a secure sandbox to reduce the effectiveness of email-borne malware.	✗	✗	✓	✗	✗	✓	Included in MS Defender for Office 365 Plans 1 & 2
Time-of-Click URL Sandboxing Scans URLs on inbound emails to check for malicious sites, reducing the threat posed by common phishing tactics.	✗	✗	Disabled by default	✗	✗	Disabled by default	Included in MS Defender for Office 365 Plans 1 & 2



The 7 protections that make or break your cyber defences

Feature	Microsoft 365 Licence						Notes
	Business Basic	Business Standard	Business Premium	E1	E3	E5	
Effective Email Threat Detection Identifies malicious emails and senders who have failed to meet verification checks and rejects emails from suspicious users.	✗	✗	✗	✗	✗	✗	High miss rate on threats - can be tuned to catch more, but results in many false positives
Email Archiving Allows emails to be stored long-term for future reference and compliance requirements.	50GB	50GB	100GB	50GB	100GB	100GB	Larger archives are possible with Exchange Online Plans 1 & 2
Conditional Access Reviews users attempting to access your environment to protect against cybercriminals using stolen credentials to access your network.	✗	✗	✓	✗	✓	✓	Included in Azure Active Directory Premium Plans 1 & 2





The 7 protections that make or break your cyber defences



1

Impersonation Protection

Microsoft's inbuilt Impersonation Protection is an AI solution which analyses email patterns between your users and their frequent contacts to try and detect impostors.

Microsoft Limitations

The AI approach Microsoft has adopted relies on having a long history of back-and-forth communications with a contact in order to make an accurate judgement, and it can only assess 350 users or 50 domains at a time - meaning for businesses in frequent contact with a range of new customers and suppliers, it offers little protection.

What's more, the AI often generates false positives, triggered by senders with common names, users emailing from personal accounts, and employees who have moved between organisations.

How Barracuda Helps

Barracuda's Impersonation Protection is included in all plans. Using the power of AI, it identifies likely impostors out of the gate, without needing a long history of communications. It also covers an unlimited number of senders and domains, perfect for fast-moving and large businesses.

2

Microsoft 365 Data Backup

While Microsoft has taken measures to reduce the risk of data losses that are due to faults on their behalf, they don't take responsibility for user error or other actions beyond their control.

Microsoft Limitations

According to Microsoft's Shared Responsibility Model, your organisation remains ultimately responsible for protecting your own data and attempting to recover assets natively in your Microsoft 365 environment can be challenging, if not impossible. Any outages can render data inaccessible and disrupt business operations.

How Barracuda Helps

With Cloud-to-Cloud Backup, Barracuda allows you to back up directly from Microsoft 365 to the cloud, giving you instant scalability and nothing to manage. To reduce risk, backups are isolated from Microsoft's production networks, and multiple secure copies of the data are maintained in different locations. Barracuda's Email Continuity service also allows you to keep an emergency inbox online to send and receive mail if your normal mail server suffers an outage, reducing the effect of any downtime.



The 7 protections that make or break your cyber defences



3

Zero-Day Attachment Sandboxing

Microsoft Safe Attachments provides an additional layer of protection for email attachments that have already been scanned by the anti-malware protection in Exchange Online Protection. By detonating attachments in a virtual environment, the solution is designed to detect zero-day threats.

Microsoft Limitations

Shared mailboxes require a license to take advantage of Safe Attachments. Microsoft uses a virtualised environment based on MS hypervisor technology to scan attachments, but many types of malware can evade this. Furthermore, shared mailboxes require a licence of their own to take advantage of Safe Attachments.

How Barracuda Helps

Barracuda Email Gateway Defense leverages multiple antivirus engines to block known malware, while unknown and zero-day threats are identified by multilayered Advanced Threat Protection, leveraging AI, heuristics, behavioural analysis, and a dynamic sandbox. While traditional sandboxes rely on a hypervisor infrastructure, Barracuda dynamically emulates different platforms to catch hypervisor-aware malware. Shared mailboxes don't require a separate license to make use of this.

4

Time-of-Click URL Sandboxing

Microsoft Safe Links helps protect against malicious links in emails. Links without a valid reputation are detonated asynchronously in the background. URLs on inbound messages are also scanned and rewritten to provide time-of-click protection for users.

Microsoft Limitations

Like Safe Attachments, Safe Links can be evaded by hypervisor-aware malware and overridden by end users. It also doesn't provide any in-the-moment security awareness to users, making ill-advised overrides more common.

How Barracuda Helps

Link Protection is included with all Barracuda Email Protection plans and requires minimal to no configuration. End users cannot override the Link Protection warning screen, and they are directed to Barracuda's Security Awareness Training. A dynamic sandbox also helps to catch hypervisor-aware malware. As with attachment sandboxing, shared mailboxes do not require their own licences.



The 7 protections that make or break your cyber defences



5

Effective Email Threat Detection

Microsoft Implicit Authentication often allows delivery from senders who haven't passed verification checks, and sometimes even blocks messages from senders who have.

Microsoft Limitations

Microsoft does not explicitly reject messages from origins that a sender has not authorised, as instructed by the sender's DMARC records. Instead, Microsoft blocks emails based on a combination of different factors. While that sounds more effective, it often results in both false negatives and false positives.

Inaccurate verdicts have to be continuously tuned out. While Microsoft claims that its own protections can successfully block 98% of malicious messages, doing so requires manual configuration to the highest possible levels of protection - levels so high that around 14% of legitimate emails get blocked, forcing IT teams to manually review and release improperly blocked mail.

How Barracuda Helps

Microsoft has a high miss rate on advanced email attacks that are caught by Barracuda Impersonation Protection. In addition, Barracuda Email Gateway Defense will reject messages from origins the sender has not authorized in their DMARC records. Barracuda doesn't override the sender's published guidance for securely accepting or rejecting emails for their domain.

6

Email Archiving

Outlook includes Microsoft Archive - a dedicated mailbox which lets user offload old email to shrink their inbox and improve performance.

Microsoft Limitations

Despite the name, Microsoft Archive often fails to act as a complete archive of emails for a business. Archive contents aren't immutable, and in order to retain deleted messages beyond a 14-day window, mailboxes have to be licenced and enabled for a litigation hold.

Archive sizes are limited, with even "unlimited" archives being capped at 1.5TB, which are automatically organised by Microsoft Purview, without room for user control. Archives are also subject to a range of restrictions, including a capped daily growth rate, maximum import size, and only allowing specific file types.

How Barracuda Helps

Barracuda's Cloud Archive Service provides truly unlimited storage on a simple and predictable per-user basis. Archive data is immutable, preventing edits made after the fact, and stored outside of production data. Archive growth is not throttled, and there are no charges to retain data in inactive mailboxes, regardless of size or the requirement for documents to be placed in litigation hold.



7 Conditional Access

Microsoft's Conditional Access combines various identity-driven signals to make decisions, enable and restrict access, and enforce organisational policies.

Microsoft Limitations

Conditional Access policies are only enforced after first-factor authentication is successful, and passwordless sign-on is unavailable. Intune is required to verify device identity, presenting challenges for users trying to access important information while on the move from a non-corporate device.

How Barracuda Helps

Barracuda offers Zero Trust Access, enhancing your multifactor authentication (MFA) implementation with certificate-based authentication in Barracuda CloudGen Access. CloudGen Access checks pairs of user and device identities before the user gets access to your systems, and, as a result, endpoint devices become an additional layer of defence against compromised Microsoft accounts, as an attacker with just credentials cannot authenticate. Secure device certificates are stored in a device's TPM or SEP modules, making them near-impossible to modify or copy.

Get Secure with Servium

If this eBook has got you thinking on your cyber defences, we should talk. As an established Barracuda partner, Servium can help you deploy all the protections necessary to close your Microsoft 365 security gaps and keep your users, data, and applications safe.

We're proud to be part of Advania, one of the largest Microsoft Gold Partners in EMEA - our experts know Microsoft 365 inside and out, and can help you assess your environment, make the most of Microsoft's native protections, and ensure that additional security seamlessly works with your business.

To learn more or discuss the solution in more detail, simply speak to your Account Manager, email us at hello@servium.com or call on +44 (0)303 334 3000.

Servium
an  advania company

 Barracuda®